Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CC-2013/09

JavaCard platform for smart card ID-One Cosmo V7.1-s on component ST23YL80C (Standard)

Paris, 29 March 2013

Courtesy Translation

SÉCURITÉ CERTIFICATION

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-2013/09

Product name

JavaCard platform for smart card ID-One Cosmo V7.1-s on component ST23YL80C (Standard)

Product reference

JavaCard Platform version: 7.1-s

Protection profile conformity

ANSSI-CC-PP-2010/03-M01 [PP JCS]

Java Card System – Open Configuration, version 3.0

Evaluation criteria and version

Common Criteria version 3.1 revision 3

Evaluation level

EAL 5 augmented

ALC_DVS.2, AVA_VAN.5

Developer(s)

Oberthur Technologies

71-73 rue des Hautes Pâtures
92726 Nanterre Cedex
France

ST Microelectronics

Smartcard IC division
190 avenue Célestin Coq
13106 Rousset
France

Sponsor

Oberthur Technologies

420 rue d'Estienne d'Orves, 92705 Colombes, France

Evaluation facility

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Recognition arrangements

CCRA

The product is recognised at EAL4 level.

SOG-IS

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, modified. This decree stipulates that:

- The French Network and Information Security Agency draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the sponsors desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Contents

1. The product

1.1. Presentation of the product

The evaluation concerns the JavaCard open platform of the product “ID-One Cosmo V7.1-s” which is a smart card which can be in contact, contactless or dual mode. The product is developed by Oberthur Technologies and masked on the microcontroller ST23YL80C (Standard) developed and manufactured by ST Microelectronics.

The JavaCard open platform is designed to supply security services to the applets which will be installed and loaded on the card.

Other applications outside the scope of this evaluation are embedded on the product (see [GUIDES]), particularly:

- the IAS ECC application designed to implement electronic signature;
- the LDS EAC application, comprising the SAC mechanism, which carries out the electronic passport functions.

1.2. Evaluated product description

1.2.1. Introduction

The security target [ST] defines the evaluated product, its evaluated security functions and its operating environment.

This security target complies with the protection profile [PP JCS]. This compliance is demonstrable.

1.2.2. Product identification

The constituent elements of the product are identified in the configuration list [CONF].

The certified version of the product can be identified by the elements contained in the response given by the product following the GET DATA command (see [GUIDES]).

The GET DATA command for the tag ‘DF 52’ gives the following responses:

Name of TOE	**ID-One Cosmo V7.1-s Standard**
Identification of microcontroller (tag ‘DF 52’, sub-tag ‘01’)	‘0C’: Standard (ST23YL80C)
Identification of mask (tag ‘DF 52’, sub-tag ‘03’)	‘61 01’ ID-One Cosmo V7.1
Identification of *Generic* patch (tag ‘DF 52’, sub-tag ‘04’) (mandatory)	‘07 97 22’ Generic r2.0 (version 00)
Identification of *SAC* patch (tag ‘DF 52’, sub-tag ‘04’) (optional)	‘07 92 12’ SAC r2 (version 02)

The *Generic* patch, loaded on the card in the pre-personalization phase (phase 5 of the life cycle), provides corrections and security improvements to the platform.

The *SAC* patch, which is loaded optionally on the card in the pre-personalization phase (phase 5 of the life cycle) at the customer’s request, provides functional corrections to the SAC mechanism (outside the evaluation). When the *SAC* patch is loaded on the card, the SAC mechanism is operational.

The GET DATA command for the tags ‘DF 66’ and ‘DF 67’ gives the following responses:

Tag ‘DF 66’ **Commercial Version of the product**	**Tag ‘DF 67’** **Internal Version of the product**
‘076651FF 07010000 0000’	‘01010F00’

The GET DATA command for the tag ‘9F 7F’ gives the following response:

- *IC Fabricator*: ST Microelectronics ‘**47 50**’;
- *IC Type*: ST23YL80C: ‘**B2 14**’;
- *Operating System Identifier*: ‘**82 31**’;
- *Operating System Release Date*: ‘**B1 5E**’;
- *Operating System Release Level*: ‘**00 75**’.

1.2.3. Security services

The main security services supplied by the product are:

- the card pre-personalization services;
- authentication of the card holder by PIN code or biometric data;
- loading, installation, deletion, extraction and integrity/authenticity checking of applets;
- supply of encryption and decryption mechanisms;
- supply of an electronic signature generation and verification mechanism;
- supply of a random number generator;
- management of the keys contained in the card (loading, generation, use, update, deletion, distribution, deactivation of use of a key, secure access and supply of an exchange protocol);

- protection of keys, PIN code, biometric data and patched code using an integrity value;
- secure processing of operations;
- supply of a *Runtime Verifier* carrying out additional checking operations during execution of applets;
- EEPROM memory management;
- firewall isolating objects or applets;
- standard GlobalPlatform services such as the logical channel and secure channels (SCP02, SCP03), together with the proprietary secure channel (SCPF3).

A detailed list of the security services is given in [ST].

The main services offered by the microcontroller are:

- initialisation of the hardware platform and attributes;
- secure life cycle management;
- logical integrity of the product;
- product tests;
- memory management (*firewall*);
- physical protection;
- security violation management;
- non-observability;
- support for cryptographic encryption;
- support for unpredictable number generation.

1.2.4. Architecture

The JavaCard platform for smart card “ID-One Cosmo V7.1-s” comprises the following components:

- the microcontroller, offering hardware functions (memory management and input/output management), and its cryptographic library;
- the BIOS, providing the interface between the native applications, such as the virtual machine, and the microcontroller;
- the resident application, in native code, enabling commands to be received from the card and distributed to the applications;
- the virtual machine interpreting the byte code of the Java applets;
- APIS, providing interfaces to the applications for key generation, key negotiation, signature and message encryption together with other proprietary programming interfaces (OT API);
- the card manager and the security domain.

This architecture is summarised in the following figure:

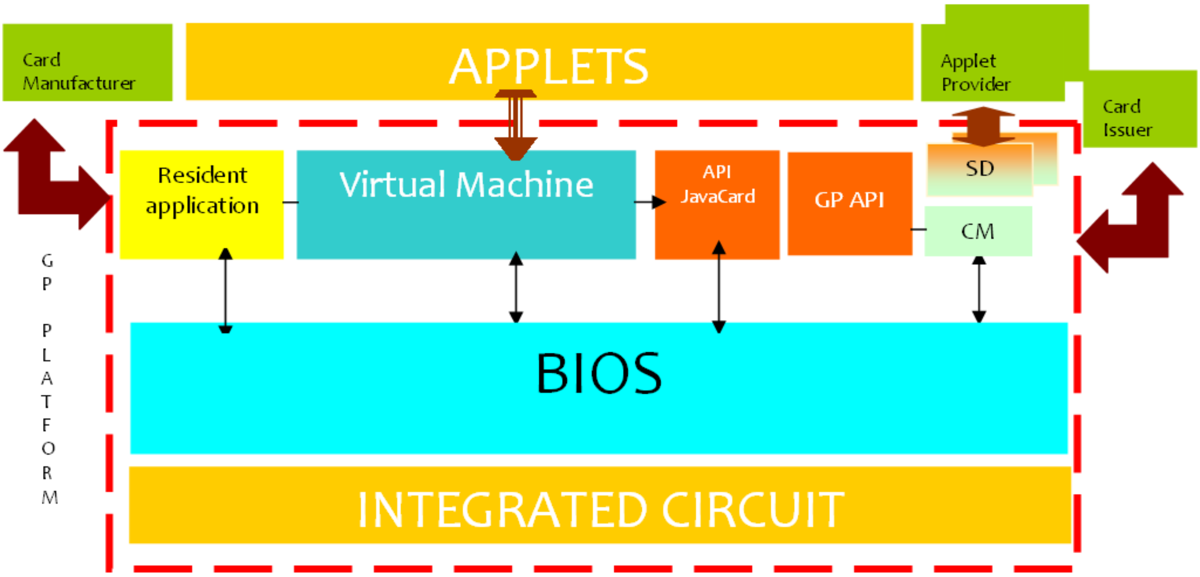

Figure 1 - TOE architecture and perimeter

1.2.5. *Life cycle*

The product's life cycle is as follows:

Phase	Phase name	Development and manufacturing sites
Phase 1	Development of embedded software	- Oberthur Technologies (*Levallois-Perret, Nanterre, Pessac*). - ID3 (*Le Fontanil-Cornillon*).
	Development of *Generic* patch and *SAC* patch	Oberthur Technologies (*Levallois-Perret, Nanterre*).
Phase 2	Development of microcontroller	ST Microelectronics.
Phase 3	Manufacturing of microcontroller	ST Microelectronics.
Phase 4	Packaging of JavaCard platform	
Phase 5	Integration of composite product. Loading of *Generic* patch (mandatory) and *SAC* patch (optional)	
Phase 6	Personalization	
Phase 7	Usage phase	

⬚ Evaluation perimeter

Figure 2 - Life cycle of JavaCard platform

With regard to the life cycle, the evaluated product is the product which comes out of the production phase (phase 3). Phases 4, 5, 6 and 7 are covered by the product guides (see [GUIDES]).

The product is developed on the following sites:

Oberthur Technologies

71-73 rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies

4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

ID3 (developer of the Match On Card function)

5 rue de la Verrerie
38120 Le Fontanil-Cornillon
France

The microcontroller is developed and manufactured by ST Microelectronics. The development and manufacturing sites for the ST23YL80C chips are detailed in the certification report with the reference [ANSSI-CC-2009/37]

1.2.6. Evaluated configuration

The certificate concerns the JavaCard open platform alone, as presented above, in paragraph "1.2.4 Architecture" and configured in accordance with the personalization guide (see [GUIDES]).

The patch loading mechanism was evaluated. This mechanism allows a functional patch to be loaded up to phase 5 of the life cycle if and only if this patch has no effect on the product's self-protection mechanisms. No patch may be loaded after phase 5, the patch loading mechanism being deactivated.

The applets embedded on the platform were analysed in this evaluation as part of the environment of the security target. They do not impair the security of the platform.

The *Match-on-Card* mechanism is incorporated in the product and enables authentication of the card holder using a digital fingerprint. The strength of this mechanism was evaluated for the default threshold values:

- *JavaCardX Security API*: 7143 (FAR = 10^{-5});
- *OTPinBio*: 10000 (FAR = 10^{-7}).

The evaluation showed that it is recommended to modify the value of the *OTPinBio* threshold by reducing it while leaving it at an acceptable level, the minimum value of the threshold being 4672 (corresponding to an FAR of $3x10^{-4}$).
The acceptable values of the threshold are therefore:

FAR (False Acceptance Rate)	Minimum value of threshold
0.03 % = 3 x 10^{-4}	4672
0.01 % = 10^{-4}	6000
0.001 % = 10^{-5}	7143
0.0001 % = 10^{-6}	8671
0.00001 % = 10^{-7}	10000 (default value of *OTPinBio*)

2. The evaluation

2.1. Evaluation referential

The evaluation was conducted in accordance with the **Common Criteria version 3.1 revision 3** [CC] and the methodology defined in the Common Evaluation Methodology [CEM] manual.

For assurance components which are not covered by the [CEM] manual, methods specific to the evaluation facility and validated by ANSSI were used.

To meet the specificities of smart cards, the [JIWG AP] guide was applied. Thus the AVA_VAN level was determined using the rating scale of the [JIWG AP] guide. This rating scale is more demanding than that defined by default in the standard method [CC] used for other categories of products (software products for example).

2.2. Evaluation work

The composition evaluation was carried out in application of the [COMP] guide to check that no weakness is introduced by the integration of the software in the microcontroller already certified.

The microcontroller ST23YL80C was certified at level EAL5 augmented by the components ALC_DVS.2 and AVA_VAN.5, in accordance with the protection profile [BSI-PP-0035-2007], on the 22nd of October 2009, under the reference [ANSSI-CC-2009/37].

The level of robustness of the microcontroller ST23YL80C was confirmed on the 27th of September as part of the monitoring process.

The evaluation technical report [ETR], submitted to ANSSI on the 21st of December 2012, details the work performed by the evaluation facility and certifies that the status of all the evaluation tasks is “**successful”**.

2.3. Cryptographic mechanisms robustness analysis

The rating of the cryptographic mechanisms was carried out in accordance with the ANSSI technical standard [REF]. The results obtained were indicated in an analysis report [ANA-CRY] and lead to the following conclusions:

- the mechanisms analysed make it possible to propose applications complying with the requirements of the ANSSI encryption standard (see [REF]);
- the GlobalPlatform specifications of the security target [ST] with which the developer is obliged to comply lead to cryptographic weaknesses. These weaknesses concern the mechanisms for protection of the sensitive data exchanged on the secure channels

SCP02 and SCP03 supported by the product. These weaknesses are also applicable to the proprietary protocol SCPF3 supported by the product.

To ensure that the mechanisms analysed comply with the requirements of the ANSSI encryption standard ([REF]), the following recommendations must be followed:

- during secure loading of applets on the card, an RSA signature using 2048-bit keys and PSS (Probabilistic Signature Scheme) encoding with the SHA-256 hash function must be used;
- the maximum number of blocks processed in the secure channel SCP02 with the same key must be less than 2^{27};
- when sensitive information is exchanged during a secure communication session, the highest level of security of the secure channel must be used (see [GUIDES]).

In any event, the results were taken into account in the independent vulnerability analysis carried out by the evaluator and did not reveal any exploitable vulnerability for the AVA_VAN.5 level targeted.

2.4. Random number generator analysis

The physical random number generator used by the end product was evaluated as part of the evaluation of the microcontroller (see [ANSSI-CC-2009/37]).
In addition, as required in the ANSSI encryption standard ([REF]), the output of the physical random number generator undergoes reprocessing of a cryptographic nature.
The results were taken into account in the independent vulnerability analysis carried out by the evaluator and did not reveal any exploitable vulnerability for the AVA_VAN.5 level targeted.

3. Certification

3.1. Conclusion

The evaluation was carried out in accordance with the rules and standards in force, with the expertise and impartiality required for an approved evaluation facility. All of the evaluation work performed permits the issuing of a certificate in accordance with decree 2002-535.

This certificate certifies that the product “JavaCard platform for smart card ID-One Cosmo V7.1-s on component ST23YL80C (Standard)” submitted for evaluation fulfils the security features specified in its security target [ST] for evaluation level EAL 5 augmented by components ALC_DVS.2 and AVA_VAN.5.

3.2. Restrictions

This certificate concerns the product specified in section 1.2 of this certification report.

The user of the certified product must make sure that the security objectives concerning the operating environment are complied with, as specified in the security target [ST], and follow the recommendations given in the guides supplied [GUIDES]. The recommendations of sections “1.2.6 Evaluated configuration” and “2.3 Rating of cryptographic mechanisms according to the ANSSI technical standard” of this report must also be implemented.

More particularly, all applications which are loaded on the card (whether certified or not) must meet all the constraints and requirements relating to the application partitioning properties imposed by the platform before they are actually installed (see [GUIDES]).

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 2010 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable, for smart cards and similar devices, up to ITSEC E6 High and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

[1] The signatory countries of the SOG-IS agreement are: Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

[2] The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Components per assurance level							Assurance level assigned to the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Component title
ADV **Development**	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD **User guides**	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC **Life cycle support**	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE **Evaluation of security target**	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE **Tests**	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample

AVA **Estimation of vulnerabilities**	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - TOUTATIS – Security Target, Reference: FQR 110 6070, version 5 of 10/12/2012, Oberthur Technologies. For publication purposes, the following security target was provided and validated in this evaluation: - Cosmo v7.1-s – TOUTATIS – Java Card Open Platform – Public Security Target, Reference: FQR 110 6155, version 1, Oberthur Technologies.
[ETR]	Evaluation Technical Report: - Evaluation Technical Report, Reference: LETI.CESTI.TOU.RTE.001, version 1.0 of 21/12/2012, CEA-LETI.
[ANA-CRY]	Rating of cryptographic mechanisms, Reference: LETI.CESTI.TOU.RT.001, version 1.0 of 16/11/2012, CEA-LETI.
[CONF]	TOUTATIS – Configuration List Reference: FQR 110 6164, version 2 of 10/12/2012 Oberthur Technologies.
[GUIDES]	- ID-One Cosmo V7.1 – Pre-Perso Guide, Reference: FQR 110 6027, version 3 of 12/12/2012, Oberthur Technologies. - ID-One Cosmo V7.1 – Reference Guide, Reference: FQR 110 6028, version 3 of 12/12/2012, Oberthur Technologies. - ID-One Cosmo V7.1 – Security Recommendations, Reference: FQR 110 6029, version 2 of 29/11/2012, Oberthur Technologies. - ID-One Cosmo V7.1 – Application Loading Protection Guidance, Reference: FQR 110 6267, version 1 of 15/11/2012, Oberthur Technologies. - Applications on ID-ONE COSMO V7.1, Reference: FQR 110 6268, version 1 of 24/09/2012, Oberthur Technologies.

	- All Applications on ID-One Cosmo V7.1, Reference: FQR 110 6319, version 1 of 25/09/2012, Oberthur Technologies.
[PP JCS]	“Java Card Protection Profile – Open Configuration”, version 3.0 of 18 May 2012. *Certified by ANSSI under the reference ANSSI-CC-PP-2010/03-M01*.
[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 August 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*
[ANSSI-CC-2009/37]	Certificate issued by ANSSI on 22 October 2009 for the product “*Secure microcontroller ST23YL80C*”.

Annex 3. Certification references

Decree number 2002-535, 18th April 2002, modified related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 3.0, 8 January 2010, Management Committee.
[REF]	Cryptographic mechanisms - Rules and recommendations concerning the choice and sizing of cryptographic mechanisms, version 1.20 of the 26th of January 2010 appended to the General Security Standard (RGS_B_1), see www.ssi.gouv.fr.